

Sharp HealthCare

Information Security Basics

Information about Sharp patients, staff, business practices and strategies, are valuable company assets. They need to be carefully managed and protected.

On our computerized systems Sharp has installed:

- Firewalls
- Anti-virus protections
- Personal user accounts
- Workstation security
- Biometric finger scan readers
- Web filters, hacker alerts and other security safeguards; however;

All the technical security that money can buy will not succeed until all network users know, understand and consistently follow basic information security practices.

This means YOU.

HIPAA requires security awareness training for all Sharp employees who have been granted accounts and access to the Sharp network and other electronic types of protected health information.

Sharp's program includes:

- Secure Password Management
- Procedures for prevention, detection and reporting malicious software (viruses)
- Procedures for monitoring and reporting evidence of unauthorized account or workstation use
- Security reminders and periodic security updates

HIPAA security regulations apply to Protected Health Information (PHI), which is managed electronically such as clinical data on:

- Computers and laptops
- Web sites and servers
- Portable devices (palm pilots)
- Computerized faxes
- Wireless devices
- Biomedical devices
- Any and all electronic devices which can view/store/process PHI

Information is considered PHI if it contains any one or more of the following data elements:

1. Names	10. Account Numbers
2. All geographic designations smaller than a state, including street addresses, city, county, zip code	11. Certificate and license numbers
3. All elements of dates (except year), including birth date, admission date, discharge date, date of death, and additional rules for ages over 89.	12. Vehicle Identifiers and serial numbers (including license plate numbers)
4. Telephone numbers	13. Device Identifiers and serial numbers.
5. Fax numbers	14. Web Universal Resource Locator (URL)
6. Electronic mail addresses	15. Internet Protocol (IP) address
7. Social Security numbers	16. Biometric identifiers (including fingerprint or voice print)
8. Medical record numbers	17. Full face photographic images and any comparable images.
9. Health plan beneficiary numbers	18. Any other unique identifying number, characteristic or code

Secure Password Management

You are the only one who knows your password.

- Your password will need to be reset if you forget it.
- Help Desk staff cannot view passwords that you have set for yourself.

To guarantee that you are the only one who knows your password:

- The system will prompt you to change your password every 90 days.
- You are encouraged to change your password more often, especially when you have used your password from a public computer external to Sharp.

Examples of secure passwords include an acronym made from a phrase or song:

YWHNB2day = Yes We Have No Bananas 2day

Or

Run short words together and add a number:

(june2thelake – or – Vegaisin05 – or – notime4weeds)

Easy to remember, hard to guess!!

Secure Workstation Management

Never leave a computer workstation unattended unless you have:

- Logged off
- Activated a privacy screen or
- Locked the computer

The automatic time-out function on your workstation is intended to be a back up measure when circumstances prevent an end-user from manually securing the workstation.

Three levels of risk have been assigned to computer workstations:

High Risk Workstations: Workstations open to or accessible by the public that are not under constant supervision, particularly workstations in secluded areas that are not easily or often monitored or workstations located in areas where the presence of non-Sharp personnel is expected, e.g. exam rooms, emergency departments, and workstations on portable cares.

Moderate Risk Workstations: Workstations in non-public areas that are difficult for the general public to access and that are supervised by Sharp staff during all hours of operations, e.g. nursing stations, intensive care units, cubicles, and administrative areas.

Minimum Risk Workstations: Workstations in private offices or lounges that are locked when unattended and are not accessible to the public.

It is risky to use a portable media, e.g. diskettes and CDs on networked workstations, unless they have been pre-scanned for viruses or other malicious code.

Software and hardware should never be installed on any networked device without knowledge and assistance from the Information Systems Department. Unauthorized installations or configuration changes may cause malfunctions immediately or during future network upgrades and patches.

Contact the Help Desk for assistance with moving devices or equipment on the network.

The World Wide Web should not be used for non-business-related streaming media, such as Internet radio stations, video, TV or interactive games. Technical Web filtering has been activated to prevent access to Web sites:

- That contain inappropriate material
- That permit downloading the background without user permission, e.g. spy ware, remote control, file shares
- That require high bandwidth
- That interfere with clinical systems

If you need access to a blocked site for Sharp **business related** reasons, call the Help Desk to request an exception.

Sharp workstations are currently being upgraded to provide additional security with some new features, including:

- Biometric finger scan devices for fast authentication
- Automated time-out on workstations when there has been no keyboard or mouse activity for a specified length of time
- Desktop and browser configurations that cannot be changed by end-users.
- New and improved shared clinical workstation to allow users to turn on or reset a workstation between users; your personal user name and password or finger scan must be entered to begin work
- The new CarePoint EMR makes it easier for a clinician to access patient data without having to open and close each application, saving time and increasing accuracy of patient data matches.

Secure Email Management

- Email is one method by which viruses may infect the Sharp network
- Be cautious about opening emailed Web links and attachments from unknown senders—
- If you are not expecting an attachment from a known sender outside of Sharp, verify that it was intentionally sent before attempting to open it.
- Do not send emails to large groups or multiple lists (more than 50 Sharp accounts). These should be submitted to Corporate Communications for review and scheduled distribution.
- When sending email that contains addresses outside of Sharp.com, place the whole distribution list in the 'blind copy' or bcc field. Click on the TO: button to use the BCC: field. Put your own address in the TO: field.

- Although the Information Systems Department email administrators have implemented measure to reduce spam and unsolicited emails, some still slip through. If you receive one, delete it and forget about it. Do not respond to the email (even to ‘unsubscribe’). This tells the sender you open and read unsolicited email...and you’ll get more.

Email is not secure!

Do not send PHI through email if it is going outside of Sharp.com unless the file is encrypted or secure.

- It can be altered and/or forwarded
- It can be spoofed or made to look like it came from someone other than the actual sender
- If forwarded or auto forwarded to an email address outside Sharp, (email address that does not end in ‘@sharp.com’) it is transmitted in clear text.
- If available, use more secure means to communicate confidential or sensitive data
- Do not send user names and passwords by email
- Do not send personal demographic data (SSN, employee IDs)
- Keep names and sensitive data out of the subject line
- Delete emails with sensitive data from your email inbox and deleted items box as soon as possible.

Secure Network Management

Manage files by deleting old duplicate or unnecessary files from your PCs F:drive. A full file server is an unavailable file server. If everyone retains only necessary files, server stability will increase. Help Desk analysts can assist you in finding efficient ways to manage your data.

Installing untested an unapproved software on Sharp workstations may interrupt the correct functioning of Sharp business and clinical applications. Certain ‘fun’ items such as some (not all) wallpaper, cursors, games and music players have hidden functionality which can expose Sharp’s confidential files and information or permit unauthorized users to access and view confidential data and files.

Please contact the Help Desk before attempting to install or configure any device which is used on the Sharp network.

Have you helped a hacker today?

Healthcare workers are in the business of being helpful. The Sharp Experience encourages us to go out of our way to assist people. *“Is there anything else I can do for you? I have the time!”*

Hackers, data thieves and information gatherers know this. A white lab coat and stethoscope or a good story by someone posing as an Information Systems department employee can convince us to provide enough information to cause a security breach.

This method of obtaining access to the network is called ‘*Social Engineering*’.

Be wise:

- Refer unusual or questionable information requests to your supervisor
- Check for an ID badge if not visible, ask to see it.
- Never disclose your username and password, even to an Information Systems Department worker; if you think someone may know it, reset a new password immediately.

Help Protect Sharp Information

Call the Help Desk if a workstation is behaving strangely or shows signs of unauthorized use.

If you use Remote Access to connect to Sharp's network, you must ensure that your home computer has active and current anti-virus software and that all security patches are applied. Sharp offers home versions of anti-virus and firewall software for all remote access users.

Make sure computer display screens cannot be viewed by patients standing at the desk or sitting in the waiting room.

Notify the Information Systems Department if a computer or laptop is missing; it may be the data on the device, not the device itself, which was the target of the theft.

Refer questions about wireless access and wireless use to the Information Systems Department. Wireless devices should be supervised and protected from unauthorized use.

If someone is asking questions about the location of the data center or other network equipment, refer the call to the Help Desk.

Facilitate Appropriate Use

If an unknown employee or clinician is demanding to receive clinical data, ask to see their ID badge.

If a patient or visitor sits down at a Sharp workstation, explain that workstations are not for public use.

Patients are permitted to use their room phone to dial-in to their internet service providers from their own laptops.

Question unknown users at workstations or contact Security at your facility to advise them of the suspicious activity.

Report inappropriate behavior to your supervisor or the Help Desk, e.g., sharing of passwords, allowing unauthorized network use, logging in for someone else.

Report any inappropriate files, pictures or Web sites to the Help Desk, if viewed on a Sharp workstation.

Acceptable Use

Sharp's Acceptable Use of Information & Computing Resources (Policy #13521) contains important information about appropriate behavior required from everyone who is granted accounts for use on the network.

Anyone who is authorized to have a computer account will be required to read and sign an agreement to follow this policy.

The behavior of every network user contributes to the overall confidentiality, data integrity and system availability of Sharp's information assets. Demonstrate your 'network citizenship' by remembering to:

- Log out of your workstation when finished
- Leave workstations secure and ready for the next user
- If you see an unattended workstation in an unsecured state, start up the privacy screen or lock the computer
- If you find **ePHI** printouts lying around, move them to a department designated inbox or escort them to the shred bin.
- If you think someone has tampered with a workstation or if you believe it may have a virus, contact the Help Desk at 858-627-5000
- If someone asks you for your password, give them the Help Desk telephone number instead

- If someone tells you their password, ask them to reset it

Computer Skills

All staff is encouraged to learn and use basic computer skills. You should know how to:

- Reset your password
- Save, find, and open files
- Use email, a web browser, and the applications required for your job
- Manage your desktop when multiple windows have been opened
- Close applications, lock the computer and/or log off
- Communicate a workstation ID and the exact text of an error message when reporting a problem to the Help Desk.

21st Century Medical Records

From one paper chart available in one place at one time to a computer file available at 9,000 workstations at the same time.

Pros

- Record available wherever patient arrives for care
- Record updates are immediately available
- Improved legibility
- Edits and audits improve patient safety

Cons

- Clinicians must acquire/use basic computing skills
- Record availability depends on system stability and ‘uptime’
- Technology evolves rapidly, more changes
- New security rules

How do the HIPAA security regs differ from the privacy regs?

HIPAA Security requirements state that Sharp and its workforce must *ensure the confidentiality, integrity, and availability of all ePHI that we:*

- Create
- Receive
- Maintain
- Transmit

Privacy is a right

Confidentiality is a condition

Security is a safeguard

Confidentiality means data or information is not made available or disclosed to unauthorized persons or processes.

Integrity means data or information has not been altered or destroyed in an unauthorized manner.

Availability means data or information is accessible and useable upon demand by an authorized person.

Sharp HealthCare
Information Security Basics
Test Questions

DATE:

(Page 1 of 2)

NAME:	TITLE:
	LICENSE #:

1. Who is responsible for information protection and data security?
 - a) The Information Systems department
 - b) The Sharp Privacy Officer and Information Security Officer
 - c) Everyone who has an account on the Sharp network
 - d) Sharp's Legal Services department

 2. What is ePHI?
 - a) Everyone's Personal Health Information
 - b) Protected Health Information which is managed electronically
 - c) The same thing we learned about in the Privacy training
 - d) A and C

 3. Passwords must be secure:
 - a) To protect Sharp information on the network
 - b) To protect my personal files and information
 - c) To prevent others from using my account
 - d) All of the above

 4. Sharp has upgraded workstations security with these new features:
 - a) Biometric finger scan devices
 - b) Automatic time-out functions
 - c) A, B and D
 - d) Re-designed shared clinical workstations

 5. E-mail users need to understand:
 - a) Appropriate use of e-mail in the workplace
 - b) Proper management of attachments and Web links from unknown senders
 - c) Policy and restrictions on use of e-mail to send ePHI to addresses outside of @sharp.com
 - d) All of the above
- Sharp HealthCare
6. The secure management of e-mail
 - a) Is part technical and part end-user behavior
 - b) Can be completely managed by technical measures
 - c) Is dependent on whether or not e-mail addresses are exposed on the Internet
 - d) Makes it private and protected

Sharp HealthCare
Information Security Basics
Test Questions

(Page 2 of 2)

7. Installing unapproved software or devices can result in:
- a) Introduction of malicious code onto the Sharp network
 - b) Incompatibilities which disrupt proper function of workstation, application or network
 - c) Exposure of Sharp's confidential files and information to unauthorized users.
 - d) All of the above
8. Who is permitted to use Sharp workstations and computer devices?
- a) Sharp workforce members who are eligible and authorized to have accounts
 - b) Visitors, patients, family members and guests who ask permission
 - c) Anyone, as long as they use SharpPC
 - d) A and B
9. Warning signs of social engineering may include:
- a) Urgent-sounding requests to use your login or to print out ePHI information
 - b) Demands to disclose your username and password
 - c) Conversations requesting information about how the network works and where the data center is located
 - d) All of the above
10. **HIPAA Privacy** regulations address confidentiality of all PHI while **HIPAA Security** regulations address
- a) Confidentiality of electronic PHI only
 - b) The right to maintain privacy of patient information
 - c) Safeguarding confidentiality, Integrity and Availability of ePHI created, received, maintained and transmitted by Sharp
 - d) None of the Above